DEPARTMENT OF THE NAVY
COMMANDER MOBILE MINE ASSEMBLY GROUP
2536 FOURTH STREET
N. CHARLESTON, S.C. 29406-6171

IN REPLY REFER TO:

COMOMAG/MOMAGINST 5230.1C CH-1
Code N01F
26 JAN 95

COMOMAG/MOMAG INSTRUCTION 5230.1C CHANGE TRANSMITTAL ONE

Subj: UTILIZATION OF AUTOMATED INFORMATION SYSTEMS (AIS)

Ref: (a) NAVELEXSECCEN 080943Z JAN 93

Encl: (1) Revised pages 13 and 14 of basic instruction

1. Purpose. To promulgate change one to the basic instruction.

2. Discussion. Following promulgation of the basic instruction, it was learned that reference (a) rescinded the use of disk overwrite utilities such as Norton Utilities' "WIPEINFO" as an approved method for declassifying magnetic media of any type. Special studies have revealed that data can still be retrieved from magnetic disk following 14 total overwrites by such routines. Presently, degaussing is the only acceptable method for clearing information from magnetic media once it has been recorded. Since degaussing is not a feasible option for hard disk drives and floppy disks are available at relatively low cost, all classified computer disks generated by MOMAG will be destroyed when they become defective or are no longer required.

3. Action. Remove pages 13 and 14 from the basic instruction and replace with enclosure (1).

D. J. POWERS

Distribution:
COMOMAG/MOMAGINST 5216.1N
List II, Case A
COMINEWARCOM (N6)

investment required to compile and/or recover such data represents a major cost in terms of money and manpower. Accordingly, all MOMAG activities will ensure the data security requirements outlined below are strictly observed.

(1) Each AIS must display a label identifying the highest classification of data which may be processed on that system.

(2) System users will ensure that no unauthorized personnel are allowed to view sensitive unclassified or classified information while it is being processed.

(3) Diskettes on which information of continuing importance is stored will contain an appropriate security classification label and be controlled in accordance with the procedures outlined in paragraph 8 of this instruction. In addition, a duplicate copy of a diskette will be made each time its data content is changed.

(4) The security and disposal measures outlined in paragraph 7(o) of this instruction will be applied to all diskettes and hard drives which contain classified data.

(5) Appropriate classification labels will be affixed to the upper and lower edges of all classified listings. These markings may be automated or may be affixed manually.

(6) Data stored on network or local (installed in an AIS) hard drives will be routinely copied to tape (backed-up) in accordance with the specifications listed below. All tapes utilized for backup procedure will be managed in accordance with paragraph 9 of this instruction.

(a) All network drives will be backed-up daily.

(b) All local drives whose data content undergo frequent modification will be backed-up each working day. Otherwise, a full backup of the local drive will be accomplished at least weekly.

o. Magnetic Media Security and Disposal. A common misconception of uneducated computer users is that data stored on magnetic storage devices can be successfully removed by reformatting the media or by deleting the files in which the data is stored. While both procedures will prevent direct access to the data, neither procedure will totally remove the data and routines exist which can be used to reconstruct deleted files and/or reformatted drives. Currently, degaussing or destruction are the only approved methods of declassifying magnetic media. Accordingly, all MOMAG activities will apply the following security and disposal procedure to magnetic media.

(1) No classified information will be stored on any fixed (non-removable) hard disk unless specifically authorized by

COMOMAG.

(2) All diskettes and all hard drives on which classified information is stored will carry a Department of the Navy (DON) magnetic media label identifying the highest classification of data stored on the device. These include:

TITLE	LABEL NUMBER
Top Secret	SF706
Secret	SF707
Confidential	SF708
Classified	SF709
Unclassified	SF710
Data Descriptor	SF711

(3) Once utilized for classified storage at a given classification level, a diskette will not be reassigned for use at a lower classification level. If the diskette is defective or is no longer required, it will be destroyed by incineration or disintegration.

(4) No hard drive on which classified information has been stored will be reassigned for use at a lower classification level or released for re-utilization. All classified hard drives which are no longer required will be destroyed in accordance with procedures outlined in paragraph 7.0.5 of this instruction or will be forwarded to COMOMAG for disposition. Disk overwrite utilities such as Norton Utilities' "WIPEINFO" will not be used in an attempt to declassify hard drives.

(5) Defective hard drives on which classified information has been stored which cannot be forwarded to a cleared repair facility or which are considered non-repairable will be destroyed in accordance with procedures outlined in reference (j). Approved procedure is:

(a) Document the material destruction in accordance with requirements specified for the classification level;

(b) Remove the drive from the system unit, open the drive and remove the disk plates;

(c) Use a grinding wheel to totally remove the surface material from both sides of the plates or drench the plates in gasoline and ignite them, or use a torch to burn the entire surface of the disk;

(d) Pulverize the plates with a sledge hammer;

(e) Dispose of the remains as unclassified waste.

p. Virus Protection. The introduction of computer viruses into the command's computer systems represents an ever